Random generation of S_n with cycle type restrictions

Daniele Garzoni
Università degli Studi di Padova

Young Researchers Algebra Conference
Napoli
17th September 2019

An old conjecture

Conjecture (Netto, 1882)

Two random elements of S_n generate either A_n or S_n with probability tending to 1 as $n \to \infty$.

In this talk, all sets/groups will be finite, and probability comes from uniform distribution.

An old conjecture

Conjecture (Netto, 1882)

Two random elements of S_n generate either A_n or S_n with probability tending to 1 as $n \to \infty$.

In this talk, all sets/groups will be finite, and probability comes from uniform distribution.

Netto's conjecture was proved almost a century later:

Theorem (Dixon, 1969)

Netto's conjecture is true.

Two related results

Theorem (Shalev, 1997)

Let $x, y \in S_n$ be chosen at random. Then, the probability that $\langle x, x^y \rangle \geqslant A_n$ tends to 1 as $n \to \infty$.

This implies Dixon's theorem, since $\langle x, x^y \rangle \leqslant \langle x, y \rangle$.

Two related results

Theorem (Shalev, 1997)

Let $x, y \in S_n$ be chosen at random. Then, the probability that $\langle x, x^y \rangle \geqslant A_n$ tends to 1 as $n \to \infty$.

This implies Dixon's theorem, since $\langle x, x^y \rangle \leqslant \langle x, y \rangle$.

Two related results

Theorem (Shalev, 1997)

Let $x, y \in S_n$ be chosen at random. Then, the probability that $\langle x, x^y \rangle \geqslant A_n$ tends to 1 as $n \to \infty$.

This implies Dixon's theorem, since $\langle x, x^y \rangle \leqslant \langle x, y \rangle$.

Two related results

Theorem (Babai-Hayes, 2006)

Let $x \in S_n$ be fixed, and let $y \in S_n$ be random. Then, $\mathbf{P}(\langle x, y\rangle \geqslant A_n) = 1 - o(1)$ if and only if x has $o(n)$ fixed points.

All asymptotic symbols (little-o, big-O...) are understood with respect to the limit $n \to \infty$.

Two related results

Theorem (Babai-Hayes, 2006)

Let $x \in S_n$ be fixed, and let $y \in S_n$ be random. Then, $\mathbf{P}(\langle x, y\rangle \geqslant A_n) = 1 - o(1)$ if and only if x has $o(n)$ fixed points.

All asymptotic symbols (little-o, big-O...) are understood with respect to the limit $n \to \infty$.

Combining the two results

Recall that $f = \Omega(g)$ if $f(n) \geq Cg(n)$ for all large enough n and for $C > 0$ absolute constant.

Theorem (S. Eberhard, DG, 2019)

Let $\pi \in S_n$ be fixed. For each j let c_j denote the number of j-cycles of π. Let π' be a random conjugate of π.

1. $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = 1 - o(1)$ if and only if $c_1 = o(n^{1/2})$ and $c_2 = o(n)$.
2. $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = \Omega(1)$ if and only if $c_1 = O(n^{1/2})$ and $c_2 = n/2 - \Omega(n)$.

Combining the two results

Recall that $f = \Omega(g)$ if $f(n) \geq Cg(n)$ for all large enough n and for $C > 0$ absolute constant.

Theorem (S. Eberhard, DG, 2019)

Let $\pi \in S_n$ be fixed. For each j let c_j denote the number of j-cycles of π. Let π' be a random conjugate of π.

1. $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = 1 - o(1)$ if and only if $c_1 = o(n^{1/2})$ and $c_2 = o(n)$.
2. $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = \Omega(1)$ if and only if $c_1 = O(n^{1/2})$ and $c_2 = n/2 - \Omega(n)$.

Combining the two results

Recall that $f = \Omega(g)$ if $f(n) \geq Cg(n)$ for all large enough n and for $C > 0$ absolute constant.

Theorem (S. Eberhard, DG, 2019)

Let $\pi \in S_n$ be fixed. For each j let c_j denote the number of j-cycles of π. Let π' be a random conjugate of π.

1. $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = 1 - o(1)$ if and only if $c_1 = o(n^{1/2})$ and $c_2 = o(n)$.
2. $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = \Omega(1)$ if and only if $c_1 = O(n^{1/2})$ and $c_2 = n/2 - \Omega(n)$.

Combining the two results

Recall that $f = \Omega(g)$ if $f(n) \geq Cg(n)$ for all large enough n and for $C > 0$ absolute constant.

Theorem (S. Eberhard, DG, 2019)

Let $\pi \in S_n$ be fixed. For each j let c_j denote the number of j-cycles of π. Let π' be a random conjugate of π.

1. $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = 1 - o(1)$ if and only if $c_1 = o(n^{1/2})$ and $c_2 = o(n)$.
2. $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = \Omega(1)$ if and only if $c_1 = O(n^{1/2})$ and $c_2 = n/2 - \Omega(n)$.

Combining the two results

Recall that $f = \Omega(g)$ if $f(n) \geq Cg(n)$ for all large enough n and for $C > 0$ absolute constant.

Theorem (S. Eberhard, DG, 2019)

Let $\pi \in S_n$ be fixed. For each j let c_j denote the number of j-cycles of π. Let π' be a random conjugate of π.

1. $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = 1 - o(1)$ if and only if $c_1 = o(n^{1/2})$ and $c_2 = o(n)$.
2. $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = \Omega(1)$ if and only if $c_1 = O(n^{1/2})$ and $c_2 = n/2 - \Omega(n)$.

The moral of the theorem is that the likelihood of $\langle \pi, \pi' \rangle \geqslant A_n$ is completely characterized by counting fixed points and 2-cycles of π.

The theorem implies Shalev's theorem mentioned earlier. Indeed:

1. Choose $x \in S_n$ at random. We may do this by picking a conjugacy class $\mathcal{C}$ with probability $|\mathcal{C}|/|S_n|$, and by picking a random element of $\mathcal{C}$.
2. It is known that with high probability x, hence $\mathcal{C}$, has very few fixed points and very few 2-cycles. Now apply the theorem.

The moral of the theorem is that the likelihood of $\langle \pi, \pi' \rangle \geqslant A_n$ is completely characterized by counting fixed points and 2-cycles of π.

The theorem implies Shalev's theorem mentioned earlier. Indeed:

1. Choose $x \in S_n$ at random. We may do this by picking a conjugacy class $\mathcal{C}$ with probability $|\mathcal{C}|/|S_n|$, and by picking a random element of $\mathcal{C}$.
2. It is known that with high probability x, hence $\mathcal{C}$, has very few fixed points and very few 2-cycles. Now apply the theorem.

The moral of the theorem is that the likelihood of $\langle \pi, \pi' \rangle \geqslant A_n$ is completely characterized by counting fixed points and 2-cycles of π.

The theorem implies Shalev's theorem mentioned earlier. Indeed:

1. Choose $x \in S_n$ at random. We may do this by picking a conjugacy class $\mathcal{C}$ with probability $|\mathcal{C}|/|S_n|$, and by picking a random element of $\mathcal{C}$.
2. It is known that with high probability x, hence $\mathcal{C}$, has very few fixed points and very few 2-cycles. Now apply the theorem.

The moral of the theorem is that the likelihood of $\langle \pi, \pi' \rangle \geqslant A_n$ is completely characterized by counting fixed points and 2-cycles of π.

The theorem implies Shalev's theorem mentioned earlier. Indeed:

1. Choose $x \in S_n$ at random. We may do this by picking a conjugacy class $\mathcal{C}$ with probability $|\mathcal{C}|/|S_n|$, and by picking a random element of $\mathcal{C}$.
2. It is known that with high probability x, hence $\mathcal{C}$, has very few fixed points and very few 2-cycles. Now apply the theorem.

Why are 1 and 2 special numbers?

Lemma

Assume G acts transitively on a set Ω. Let $\pi \in G$ be fixed, and let π' be a random conjugate of π. Assume π has k fixed points on Ω. Then

$$\mathbf{P}(\mathrm{fix}(\pi) \cap \mathrm{fix}(\pi') \neq \emptyset) \leqslant \mathbf{E}(\mathrm{fix}(\pi) \cap \mathrm{fix}(\pi')) = k^2/|\Omega|.$$

We now apply this to some cases of interest to us.

Why are 1 and 2 special numbers?

Lemma

Assume G acts transitively on a set Ω. Let $\pi \in G$ be fixed, and let π' be a random conjugate of π. Assume π has k fixed points on Ω. Then

$$\mathbf{P}(\mathrm{fix}(\pi) \cap \mathrm{fix}(\pi') \neq \emptyset) \leqslant \mathbf{E}(\mathrm{fix}(\pi) \cap \mathrm{fix}(\pi')) = k^2/|\Omega|.$$

We now apply this to some cases of interest to us.

Why are 1 and 2 special numbers?

Lemma

Assume G acts transitively on a set Ω. Let $\pi \in G$ be fixed, and let π' be a random conjugate of π. Assume π has k fixed points on Ω. Then

$$\mathbf{P}(\mathrm{fix}(\pi) \cap \mathrm{fix}(\pi') \neq \emptyset) \leqslant \mathbf{E}(\mathrm{fix}(\pi) \cap \mathrm{fix}(\pi')) = k^2/|\Omega|.$$

We now apply this to some cases of interest to us.

Why are 1 and 2 special numbers?

The natural action of S_n on n points.

- Then $k = c_1$, and $k^2/|\Omega| = c_1^2/n$.
- By the previous lemma, the probability that π and π' have a common fixed points is at most the expected number of common fixed points, which is c_1^2/n.
- If $\langle \pi, \pi' \rangle \geqslant A_n$, then certainly π and π' do not fix a common point.
- Therefore we expect to need the condition $c_1 = o(n^{1/2})$.

Why are 1 and 2 special numbers?

The natural action of S_n on n points.

- Then $k = c_1$, and $k^2/|\Omega| = c_1^2/n$.
- By the previous lemma, the probability that π and π' have a common fixed points is at most the expected number of common fixed points, which is c_1^2/n.
- If $\langle \pi, \pi' \rangle \geqslant A_n$, then certainly π and π' do not fix a common point.
- Therefore we expect to need the condition $c_1 = o(n^{1/2})$.

Why are 1 and 2 special numbers?

The natural action of S_n on n points.

- Then $k = c_1$, and $k^2/|\Omega| = c_1^2/n$.
- By the previous lemma, the probability that π and π' have a common fixed points is at most the expected number of common fixed points, which is c_1^2/n.
- If $\langle \pi, \pi' \rangle \geqslant A_n$, then certainly π and π' do not fix a common point.
- Therefore we expect to need the condition $c_1 = o(n^{1/2})$.

Why are 1 and 2 special numbers?

The natural action of S_n on n points.

- Then $k = c_1$, and $k^2/|\Omega| = c_1^2/n$.
- By the previous lemma, the probability that π and π' have a common fixed points is at most the expected number of common fixed points, which is c_1^2/n.
- If $\langle \pi, \pi' \rangle \geqslant A_n$, then certainly π and π' do not fix a common point.
- Therefore we expect to need the condition $c_1 = o(n^{1/2})$.

Why are 1 and 2 special numbers?

With very similar computations, one sees that:

- The expected number of common fixed 2-sets of π and π' is small if and only if $c_1 = o(n^{1/2})$ and $c_2 = o(n)$.
- The expected number of common fixed 3-sets of π and π' is small anyway!

Why are 1 and 2 special numbers?

With very similar computations, one sees that:

- The expected number of common fixed 2-sets of π and π' is small if and only if $c_1 = o(n^{1/2})$ and $c_2 = o(n)$.
- The expected number of common fixed 3-sets of π and π' is small anyway!

Some remarks on the “only if” part

Warning

So far we have proved nothing!

- For the “only if” part, the fact that the expectation is large does not imply that the probability is large!
  (A little argument is sufficient for almost-sure generation.)
- Regarding positive-probability generation, surprising (to us) that if $c_2 = n/2 - o(n)$, i,e., if π is close to be a product of 2-cycles, then $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) \to 0$.
  (Proof uses second moment method.)

Some remarks on the “only if” part

Warning

So far we have proved nothing!

- For the “only if” part, the fact that the expectation is large does not imply that the probability is large!
  (A little argument is sufficient for almost-sure generation.)
- Regarding positive-probability generation, surprising (to us) that if $c_2 = n/2 - o(n)$, i,e., if π is close to be a product of 2-cycles, then $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) \to 0$.
  (Proof uses second moment method.)

Some remarks on the “only if” part

Warning

So far we have proved nothing!

- For the “only if” part, the fact that the expectation is large does not imply that the probability is large!
(A little argument is sufficient for almost-sure generation.)
- Regarding positive-probability generation, surprising (to us) that if $c_2 = n/2 - o(n)$, i,e., if π is close to be a product of 2-cycles, then $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) \to 0$.
(Proof uses second moment method.)

Some remarks on the “only if” part

Warning

So far we have proved nothing!

- For the “only if” part, the fact that the expectation is large does not imply that the probability is large!
  (A little argument is sufficient for almost-sure generation.)
- Regarding positive-probability generation, surprising (to us) that if $c_2 = n/2 - o(n)$, i,e., if π is close to be a product of 2-cycles, then $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) \to 0$.
  (Proof uses second moment method.)

A brief sketch of proof of the "if" part

1. Proof divided with respect to transitive and intransitive subgroups. Core of the proof is the intransitive case.
2. Define N to be the random variable which counts the number of subsets of $\{1, 2, \ldots, n\}$ on which $\langle \pi, \pi' \rangle$ acts transitively.
3. We show that if $c_1 = o(n^{1/2})$ and $c_2 = o(n)$ then $\mathbf{E}(N) = o(1)$, hence $\langle \pi, \pi' \rangle$ is almost surely transitive.
4. We show that if $c_1 = O(n^{1/2})$ and $c_2 = n/2 - \Omega(n)$ then $\mathbf{E}(N) = O(1)$.
5. We then use the method of moments to show the Poisson-type approximation $\mathbf{P}(N = 0) = e^{-\mathbf{E}(N)} + o(1)$, hence $\langle \pi, \pi' \rangle$ is transitive with positive probability.

A brief sketch of proof of the "if" part

1. Proof divided with respect to transitive and intransitive subgroups. Core of the proof is the intransitive case.
2. Define N to be the random variable which counts the number of subsets of $\{1, 2, \ldots, n\}$ on which $\langle \pi, \pi' \rangle$ acts transitively.
3. We show that if $c_1 = o(n^{1/2})$ and $c_2 = o(n)$ then $\mathbf{E}(N) = o(1)$, hence $\langle \pi, \pi' \rangle$ is almost surely transitive.
4. We show that if $c_1 = O(n^{1/2})$ and $c_2 = n/2 - \Omega(n)$ then $\mathbf{E}(N) = O(1)$.
5. We then use the method of moments to show the Poisson-type approximation $\mathbf{P}(N = 0) = e^{-\mathbf{E}(N)} + o(1)$, hence $\langle \pi, \pi' \rangle$ is transitive with positive probability.

A brief sketch of proof of the “if” part

1. Proof divided with respect to transitive and intransitive subgroups. Core of the proof is the intransitive case.
2. Define N to be the random variable which counts the number of subsets of $\{1, 2, \ldots, n\}$ on which $\langle \pi, \pi' \rangle$ acts transitively.
3. We show that if $c_1 = o(n^{1/2})$ and $c_2 = o(n)$ then $\mathbf{E}(N) = o(1)$, hence $\langle \pi, \pi' \rangle$ is almost surely transitive.
4. We show that if $c_1 = O(n^{1/2})$ and $c_2 = n/2 - \Omega(n)$ then $\mathbf{E}(N) = O(1)$.
5. We then use the method of moments to show the Poisson-type approximation $\mathbf{P}(N = 0) = e^{-\mathbf{E}(N)} + o(1)$, hence $\langle \pi, \pi' \rangle$ is transitive with positive probability.

A brief sketch of proof of the "if" part

1. Proof divided with respect to transitive and intransitive subgroups. Core of the proof is the intransitive case.
2. Define N to be the random variable which counts the number of subsets of $\{1, 2, \dots, n\}$ on which $\langle \pi, \pi' \rangle$ acts transitively.
3. We show that if $c_1 = o(n^{1/2})$ and $c_2 = o(n)$ then $\mathbf{E}(N) = o(1)$, hence $\langle \pi, \pi' \rangle$ is almost surely transitive.
4. We show that if $c_1 = O(n^{1/2})$ and $c_2 = n/2 - \Omega(n)$ then $\mathbf{E}(N) = O(1)$.
5. We then use the method of moments to show the Poisson-type approximation $\mathbf{P}(N = 0) = e^{-\mathbf{E}(N)} + o(1)$, hence $\langle \pi, \pi' \rangle$ is transitive with positive probability.

Applications

1. Whenever one picks random elements from a normal subset of S_n, one can apply the theorem (a more general version of it!)
2. For example, we answered to the following question: For which integers m two random elements of order m generate S_n with high (positive) probability?

Applications

1. Whenever one picks random elements from a normal subset of S_n, one can apply the theorem (a more general version of it!)
2. For example, we answered to the following question: For which integers m two random elements of order m generate S_n with high (positive) probability?

Theorem (S. Eberhard, DG, 2019)

Let $m \in \mathrm{ord}(S_n)$, and assume that either

1. m has a divisor d in the range $3 \leqslant d \leqslant o(n^{1/2})$, or
2. m is even and there is at least one $\pi \in S_n$ of order m with $o(n^{1/2})$ fixed points and $o(n)$ 2-cycles.

Then two random elements of S_n of order m almost surely generate at least A_n.

Theorem (S. Eberhard, DG, 2019)

Let $m \in \mathrm{ord}(S_n)$. Then two random elements of order m generate at least A_n with probability bounded away from zero if and only if

1. m is odd and there is at least one $\pi \in S_n$ of order m with $O(n^{1/2})$ fixed points, or
2. m is even and not 2.

Theorem (S. Eberhard, DG, 2019)

Let $m \in \mathrm{ord}(S_n)$, and assume that either

1. m has a divisor d in the range $3 \leqslant d \leqslant o(n^{1/2})$, or
2. m is even and there is at least one $\pi \in S_n$ of order m with $o(n^{1/2})$ fixed points and $o(n)$ 2-cycles.

Then two random elements of S_n of order m almost surely generate at least A_n.

Theorem (S. Eberhard, DG, 2019)

Let $m \in \mathrm{ord}(S_n)$. Then two random elements of order m generate at least A_n with probability bounded away from zero if and only if

1. m is odd and there is at least one $\pi \in S_n$ of order m with $O(n^{1/2})$ fixed points, or
2. m is even and not 2.

Thank you!